ZAP by Checkmarx Scanning Report

Sites: https://127.0.0.1:5000 http://127.0.0.1:5000

Generated on Wed, 18 Jun 2025 09:33:57

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	7
Medium	4
Low	7
Informational	15
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause	High	3
Cross Site Scripting (Reflected)	High	3
LDAP Injection - openldap	High	1
NoSQL Injection - MongoDB	High	1
Path Traversal	High	7
SQL Injection	High	8
Source Code Disclosure - File Inclusion	High	2
Content Security Policy (CSP) Header Not Set	Medium	1
Format String Error	Medium	1
HTTP Only Site	Medium	1
Integer Overflow Error	Medium	1
Application Error Disclosure	Low	1
Cross Site Scripting Weakness (Persistent in JSON Response)	Low	1
Full Path Disclosure	Low	1
Insufficient Site Isolation Against Spectre Vulnerability	Low	21
Permissions Policy Header Not Set	Low	2
Server Leaks Version Information via "Server"		

HTTP Response Header Field	Low	60
X-Content-Type-Options Header Missing	Low	17
Authentication Request Identified	Informational	4
Base64 Disclosure	Informational	2
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	1
Non-Storable Content	Informational	16
Sec-Fetch-Dest Header is Missing	Informational	60
Sec-Fetch-Mode Header is Missing	Informational	60
Sec-Fetch-Site Header is Missing	Informational	60
Sec-Fetch-User Header is Missing	Informational	60
Session Management Response Identified	Informational	6
Storable and Cacheable Content	Informational	47
Storable but Non-Cacheable Content	Informational	3
Tech Detected - Flask	Informational	2
Tech Detected - Python	Informational	2
User Agent Fuzzer	Informational	105

Alert Detail

High	**Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause**
Description	A SQL injection may be possible using the attached payload.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	hacker book) AND 5148=5148 AND (3504=3504
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [hacker book) AND 5148=5148 AND (3504=3504] and [hacker book) AND 4625=9434 AND (3721=3721] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Hacker) AND 9726=9726 AND (2039=2039
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [Hacker) AND 9726=9726 AND (2039=2039] and [Hacker) AND 1323=5383 AND (4513=4513] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	hacker2) AND 2983=2983 AND (6187=6187
Evidence	
	The page results were successfully manipulated using the boolean conditions [hacker2)

Other Info	AND 2983=2983 AND (6187=6187] and [hacker2) AND 8559=6428 AND (1266=1266] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
Instances	3
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the privilege of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	90018

High	**Cross Site Scripting (Reflected)**
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML /JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In

	such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	'"<scrIpt>alert(1);</scRipt>
Evidence	'"<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	'"<scrIpt>alert(1);</scRipt>
Evidence	'"<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
Other Info	
Instances	3
	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-

Solution	side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40012

High	**LDAP Injection - openldap**
Description	LDAP Injection may be possible. It may be possible for an attacker to bypass authentication controls, and to view and modify arbitrary data in the LDAP directory.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	parameter [book_title] set to [|!<>=~=>=<=*(),+-'"\/]
Evidence	Already exists
Other Info	parameter [book_title] on [POST] [http://127.0.0.1:5000/books/v1] may be vulnerable to LDAP injection, using an attack with LDAP meta-characters [|!<>=~=>=<=*(),+-'"\/], yielding known [openldap] error message [Already exists], which was not present in the original response.
Instances	1

Solution	Validate and/or escape all user input before using it to create an LDAP query. In particular, the following characters (or combinations) should be deny listed: & | ! < > = ~= >= <= * ( ) , + - " ' ; \ / NUL character
Reference	https://owasp.org/www-community/attacks/LDAP_Injection https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html
CWE Id	90
WASC Id	29
Plugin Id	40015

High	**NoSQL Injection - MongoDB**
Description	MongoDB query injection may be possible.
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	$regex.*
Evidence	
Other	In some NodeJS based back end implementations, messages having the JSON format as content-type are expected. In order to obtain sensitive data it is possible to attack these

Info	applications injecting the "{$ne:}" string (or other similar ones) that is processed as an associative array rather than a simple text. Through this, the queries made to MongoDB will always be true.
Instances	1
Solution	Do not trust client side input and escape all data on the server side. Avoid to use the query input directly into the where and group clauses and upgrade all drivers at the latest available version.
Reference	https://arxiv.org/pdf/1506.04082.pdf https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05.6-Testing_for_NoSQL_Injection.html
CWE Id	943
WASC Id	19
Plugin Id	40033

High	**Path Traversal**
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding ("..%255c") of the backslash character. Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable script. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.
URL	http://127.0.0.1:5000/books/v1?__debugger__=%2Fv1&cmd=resource&f=debugger.js
Method	GET
Attack	/v1
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	createdb
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	/v1
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	\v1
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	v1
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	/login
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	register
Evidence	
Other Info	
Instances	7
	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent allow lists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exclude directory separators such as "/". Use an allow list of allowable file extensions.

Solution	Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass allow list schemes by introducing dangerous inputs after they have been checked. Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links. Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	https://owasp.org/www-community/attacks/Path_Traversal https://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Plugin Id	6

High	**SQL Injection**
Description	SQL injection may be possible.
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP+AND+1%3D1+--+
Method	GET
Attack	ZAP AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [ZAP AND 1=1 --] and [ZAP AND 1=2 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin+AND+1%3D1+--+&pin=ZAP
Method	GET
Attack	Confirm Pin OR 1=1 --
Evidence	

Other Info	The page results were successfully manipulated using the boolean conditions [Confirm Pin AND 1=1 --] and [Confirm Pin OR 1=1 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was NOT returned for the original parameter. The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	hacker book' OR '1'='1' --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [hacker book' AND '1'='1' --] and [hacker book' OR '1'='1' --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was NOT returned for the original parameter. The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	hacker@ime.eb.br AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [hacker@ime.eb.br AND 1=1 --] and [hacker@ime.eb.br AND 1=2 --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	teste@email.com" AND "1"="1" --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [teste@email.com" AND "1"="1" --] and [teste@email.com" AND "1"="2" --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	123458-2
Evidence	
Other Info	The original page results were successfully replicated using the expression [123458-2] as the parameter value The parameter value being modified was stripped from the HTML output for the purposes of the comparison.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	123456' AND '1'='1' --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [123456' AND '1'='1' --] and [123456' AND '1'='2' --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST

Attack	teste AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [teste AND 1=1 --] and [teste AND 1=2 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.
Instances	8
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

High	**Source Code Disclosure - File Inclusion**
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e% 2e%2f"), and double URL encoding ("..%255c") of the backslash character.

	Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable script. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	v1
Evidence	
Other Info	The output for the source code filename [v1] differs sufficiently from that of the random parameter [sydkxyzytdiwszasfflijvepadpfvpaskmouqe], at [0%], compared to a threshold of [75%]
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	register
Evidence	
Other Info	The output for the source code filename [register] differs sufficiently from that of the random parameter [sydkxyzytdiwszasfflijvepadpfvpaskmouqe], at [0%], compared to a threshold of [75%]
Instances	2
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent allow lists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exclude directory separators such as "/". Use an allow list of allowable file extensions. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass allow list schemes by introducing dangerous inputs after they have been checked. Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links.

	Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	https://owasp.org/www-community/attacks/Path_Traversal https://cwe.mitre.org/data/definitions/22.html
CWE Id	541
WASC Id	33
Plugin Id	43

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Format String Error**

Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	ZAP %1!s%2!s%3!s%4!s%5!s%6!s%7!s%8!s%9!s%10!s%11!s%12!s%13!s%14!s%15!s%16!s%17!s%18!s%19!s%20!s%21!n%22!n%23!n%24!n%25!n%26!n%27!n%28!n%29!n%30!n%31!n%32!n%33!n%34!n%35!n%36!n%37!n%38!n%39!n%40!n
Evidence	
Other Info	Potential Format String Error. The script closed the connection on a Microsoft format string error.
Instances	1
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Reference	https://owasp.org/www-community/attacks/Format_string_attack
CWE Id	134
WASC Id	6
Plugin Id	30002

Medium	**HTTP Only Site**
Description	The site is only served under HTTP and not HTTPS.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	Failed to connect. ZAP attempted to connect via: https://127.0.0.1:5000/books/v1
Instances	1
Solution	Configure your web or application server to use SSL (https).
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html https://letsencrypt.org/
CWE Id	311
WASC Id	4
Plugin Id	10106

Medium	**Integer Overflow Error**
Description	An integer overflow condition exists when an integer used in a compiled program extends beyond the range limits and has not been properly checked from the input stream.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	1111111111111111111111111111111111111111
Evidence	HTTP/1.1 500 INTERNAL SERVER ERROR
Other Info	Potential Integer Overflow. Status code changed on the input of a long string of ones.
Instances	1
Solution	In order to prevent overflows and divide by 0 (zero) errors in the application, please rewrite the backend program, checking if the values of integers being processed are within the application's allowed range. This will require a recompilation of the backend executable.

Reference	https://en.wikipedia.org/wiki/Integer_overflow https://cwe.mitre.org/data/definitions/190.html
CWE Id	190
WASC Id	3
Plugin Id	30003

Low	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	HTTP/1.1 500 INTERNAL SERVER ERROR
Other Info	
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	550
WASC Id	13
Plugin Id	90022

Low	**Cross Site Scripting Weakness (Persistent in JSON Response)**
Description	A XSS attack was found in a JSON response, this might leave content consumers vulnerable to attack if they don't appropriately handle the data (response).
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	<script>alert(1);</script>
Evidence	
Other Info	Raised with LOW confidence as the Content-Type is not HTML.
Instances	1
	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

Solution	For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40014

Low	**Full Path Disclosure**
Description	The full path of files which might be sensitive has been exposed to the client.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	

Evidence	/home/
Other Info	
Instances	1
Solution	Disable directory browsing in your web server. Refer to the web server documentation.
Reference	https://owasp.org/www-community/attacks/Full_Path_Disclosure
CWE Id	209
WASC Id	13
Plugin Id	110009

Low	**Insufficient Site Isolation Against Spectre Vulnerability**
Description	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js

Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	PUT
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	
Other Info	
Instances	21
Solution	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided. If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low	**Permissions Policy Header Not Set**
Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/feature-policy/ https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/

CWE Id	693
WASC Id	15
Plugin Id	10063

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png

Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/debug
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/favicon.ico
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home
Method	GET
Attack	

Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views/books.py
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models/books_model.py
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14

Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/decorator.py
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/parameter.py
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14

Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/uri_parsing.py
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/robots.txt
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	

URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/debug
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password

Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	GET
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	GET
Attack	

Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	POST
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14

Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	PUT
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	Werkzeug/2.2.3 Python/3.10.14
Other Info	
Instances	60
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	17
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	password

Other Info	userParam=username userValue=admin passwordParam=password
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=hacker passwordParam=password
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=name1 passwordParam=password
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=teste de usuario passwordParam=password
Instances	4
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Base64 Disclosure**
Description	Base64 encoded data was disclosed by the application/web server. Note: in the interests of performance not all base64 strings in the response were analyzed individually, the entire response should be looked at by the analyst/security team/developer(s).
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	/home/kali/VAmPI/venv310/lib/python3
Other Info	\x001a&{\x001a/\x0002c}tX
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
Other Info	{"alg":"HS256","typ":"JWT"}
Instances	2
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data cannot be aggregated/used to exploit other vulnerabilities.

Reference	https://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	319
WASC Id	13
Plugin Id	10094

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// Prevent page from refreshing.", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "<!-- Traceback (most recent call last): File "/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py", line 2548,", see evidence field for the suspicious comment/snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	<script src="?__debugger__=yes&cmd=resource&f=debugger.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Non-Storable Content**

Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	
Evidence	DELETE
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	
Evidence	DELETE
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	500
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	authorization:
Other Info	
URL	http://127.0.0.1:5000/debug
Method	GET
Attack	
Evidence	authorization:
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	authorization:
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	authorization:
Other	

Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	POST
Attack	
Evidence	authorization:
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	400
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	authorization:
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	
Evidence	PUT
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	
Evidence	PUT
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	PUT
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	PUT
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email

Method	PUT
Attack	
Evidence	PUT
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	PUT
Other Info	
Instances	16
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	**Sec-Fetch-Dest Header is Missing**
Description	Specifies how and where the data would be used. For instance, if the value is audio, then the requested resource must be audio data and not any other type of resource.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali
Method	GET
Attack	
Evidence	
Other Info	

URL	http://127.0.0.1:5000/home/kali/VAmPI
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views/books.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models/books_model.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/decorator.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/parameter.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/uri_parsing.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask

Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	GET
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	

URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	PUT

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	
Other Info	
Instances	60
Solution	Ensure that Sec-Fetch-Dest header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Dest
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	**Sec-Fetch-Mode Header is Missing**
Description	Allows to differentiate between requests for navigating between HTML pages and requests for loading resources like images, audio etc.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books

Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/debug
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views/books.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models
Method	GET
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models/books_model.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/decorator.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/parameter.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/uri_parsing.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/users
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker

Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	
Other Info	
Instances	60
Solution	Ensure that Sec-Fetch-Mode header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Mode
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	**Sec-Fetch-Site Header is Missing**
Description	Specifies the relationship between request initiator's origin and target's origin.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI

Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views/books.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models/books_model.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/decorator.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/parameter.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/uri_parsing.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login

Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	PUT

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	
Other Info	
Instances	60
Solution	Ensure that Sec-Fetch-Site header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Site
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	**Sec-Fetch-User Header is Missing**
Description	Specifies if a navigation request was initiated by a user.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books

Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/debug
Method	GET
Attack	

Evidence	
Other Info	
URL	http://127.0.0.1:5000/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views/books.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models
Method	GET
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/models/books_model.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators
Method	GET
Attack	
Evidence	
Other Info	

URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/decorator.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/parameter.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/uri_parsing.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	

URL	http://127.0.0.1:5000/users
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/debug
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	PUT
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	PUT
Attack	
Evidence	
Other Info	
Instances	60
Solution	Ensure that Sec-Fetch-User header is included in user initiated requests.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-User
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://127.0.0.1:5000/users/v1/login
Method	DELETE

Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJleHAiOjE3NTExOTU4MTUsImlhdCI6MTc1MDE5NTgxNiwic3ViIjoiYWRtaW4ifQ. AjJDwDC1P6-SFjqgHD8BUyuyEFoCgcWL_q7Lv21pNIE
Other Info	json:auth_token
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJleHAiOjE3NTExOTc1MTEsImlhdCI6MTc1MDE5NzUxMiwic3ViIjoibmFtZTEifQ. o96DXjlPmQzwIZyH3oAPVMQp_yPs8rs8wTwxkj-TsRQ
Other Info	json:auth_token
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJleHAiOjE3NTExOTU4MTUsImlhdCI6MTc1MDE5NTgxNiwic3ViIjoiYWRtaW4ifQ. AjJDwDC1P6-SFjqgHD8BUyuyEFoCgcWL_q7Lv21pNIE
Other Info	json:auth_token
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJleHAiOjE3NTExOTc1MTEsImlhdCI6MTc1MDE5NzUxMiwic3ViIjoibmFtZTEifQ. o96DXjlPmQzwIZyH3oAPVMQp_yPs8rs8wTwxkj-TsRQ
Other Info	json:auth_token
URL	http://127.0.0.1:5000/users/v1/login
Method	PUT
Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJleHAiOjE3NTExOTU4MTUsImlhdCI6MTc1MDE5NTgxNiwic3ViIjoiYWRtaW4ifQ. AjJDwDC1P6-SFjqgHD8BUyuyEFoCgcWL_q7Lv21pNIE
Other Info	json:auth_token
URL	http://127.0.0.1:5000/users/v1/login
Method	PUT
Attack	
Evidence	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJleHAiOjE3NTExOTc1MTEsImlhdCI6MTc1MDE5NzUxMiwic3ViIjoibmFtZTEifQ. o96DXjlPmQzwIZyH3oAPVMQp_yPs8rs8wTwxkj-TsRQ
Other Info	json:auth_token
Instances	6
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

Informational	**Storable and Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	http://127.0.0.1:5000
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/books
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/createdb
Method	GET

Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/debug
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/api_views/books.py
Method	GET
Attack	
Evidence	

Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/models
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/models/books_model.py
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/decorator.py
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/parameter.py
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/connexion/decorators/uri_parsing.py
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/home/kali/VAmPI/venv310/lib/python3.10/site-packages/flask/app.py
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

URL	http://127.0.0.1:5000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/_debug
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/admin
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/debug

Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/hacker
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/hacker/password
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/login
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/name1
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/name1/email
Method	GET
Attack	

Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/name2
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/name2/email
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/register
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Instances	47
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
	https://datatracker.ietf.org/doc/html/rfc7234

Reference	https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	Storable but Non-Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=console.png
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=debugger.js
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	http://127.0.0.1:5000/books/v1?__debugger__=yes&cmd=resource&f=style.css
Method	GET
Attack	
Evidence	no-cache
Other Info	
Instances	3
Solution	
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	Tech Detected - Flask
Description	The following "Web frameworks, Web servers" technology was identified: Flask. Described as: Flask is a Python micro web framework ideal for rapidly constructing web applications, offering minimalism, flexibility, and modularity.
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	Werkzeug/2.2.3

Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:palletsprojects:flask:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 2.2.3
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	Werkzeug/2.2.3
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:palletsprojects:flask:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 2.2.3
Instances	2
Solution	
Reference	https://github.com/pallets/flask/
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Python**
Description	The following "Programming languages" technology was identified: Python. Described as: Python is an interpreted and general-purpose programming language.
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	
Evidence	Python/3.10.14
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:python:python:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 3.10.14
URL	http://127.0.0.1:5000/users/v1/login
Method	POST
Attack	
Evidence	Python/3.10.14
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:python:python:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 3.10.14
Instances	2
Solution	
Reference	https://python.org
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	

Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker2
Method	DELETE
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	

Other Info	
URL	http://127.0.0.1:5000/users/v1/name2
Method	DELETE
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other	

Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1?btn=Confirm+Pin&pin=ZAP
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/createdb
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1

Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/books/v1
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register

Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/register
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT

Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/email
Method	PUT
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Attack	Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/admin/password
Method	PUT

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0

Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://127.0.0.1:5000/users/v1/hacker/email
Method	PUT
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	105
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104